UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,919	08/02/2001	Kaijun Tan	230074-0238	7139

7590 11/30/2004

Ted R. Rittmaster
FOLEY & LARDNER
Suite 3500
2029 Century Park East
Los Angeles, CA 90067-3021

EXAMINER	
HOSSAIN, TANIM M	

ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,919	TAN ET AL.	
	Examiner	Art Unit	
	Tanim Hossain	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) 1-32 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 8/2/01 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 10282004.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim 27 is objected to because of the following informalities: The claim upon which claim 27 depends has been misnumbered as claim 22, when it appears to be consistent with claim 23. Appropriate correction is required.

Claim Rejections - 35 USC § 103

Claims 1-29, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper (U.S. 2001/0051996) in view of Williams (U.S. 2002/0002541).

As per claim 1, Cooper teaches a method for distributing data over a network comprising: issuing a certificate and a private key to a client for identifying the client in a transaction (page 2, paragraph 0018; page 3, paragraph 0042); verifying a digital signature using the certificate before distributing data to the client (page 2, paragraph 0019); generating a message associated with the data being downloaded to the client and associated with the user's private key (page 8, paragraph 0102); and distributing the data and the associated message to the client (page 8, paragraph 0110). Cooper does not specifically teach the storage of the private key and digital certificate on a token. Williams teaches the storage of key and certificate information on a token, or cookie (page 3, paragraph 0042). It would have been obvious to one of ordinary skill in the art to include the ability of the key and certificate to be stored on a token, as taught by Williams

in the system of Cooper. The motivation for doing so lies in the fact that the storage of the key and certificate on a cookie would bypass login procedures for future use, allowing for ease of use. Both inventions are from the same field of endeavor, namely the reliable transmittal of data files over a network.

As per claim 2, Cooper-Williams teaches the method of claim 1, further comprising providing the client with information necessary for establishing an account (Cooper: page 8, paragraph 0126).

As per claim 3, Cooper-Williams teaches the method of claim 2, further comprising providing the client with the token (Cooper: page 2, paragraph 0019; where the authentication of the certificate given by the user constitutes providing the client with the token, in light of the treatment of claim 1).

As per claim 4, Cooper-Williams teaches a method for distributing data over a network comprising: establishing a secure connection between a client and a server (Cooper: page 2, paragraph 0032); issuing a certificate and the private key to the client for identifying the client in a transaction (page 2, paragraph 0018); and storing the certificate and the private key in a token used by the client during a transaction (Cooper: page 2, paragraph 0018; Williams: page 5, paragraph 0042).

As per claim 5, Cooper-Williams teaches the method of claim 4, further comprising distributing data to the client (Cooper: page 2, paragraph 0019).

As per claim 6, Cooper-Williams teaches the method of claim 5, further comprising requesting information from the client for establishing an account (Cooper: page 8, paragraph 0126).

As per claim 7, Cooper-Williams teaches the method of claim 4, wherein establishing a secure connection comprises establishing a secure connection using a security protocol (Cooper: page 2, paragraph 0032).

As per claim 8, Cooper-Williams teaches the method of claim 7, wherein the security protocol is the secure socket layer protocol (Cooper: page 2, paragraph 0032).

As per claim 9, Cooper-Williams teaches the method of claim 6, wherein the requesting information comprises requesting a credit card number (Cooper: page 8, paragraph 0126).

As per claim 10, Cooper-Williams teaches the method of claim 6, wherein requesting information comprises requesting a password (Cooper: page 8, paragraph 0126).

As per claim 11, Cooper-Williams teaches the method of claim 4, wherein storing the certificate comprises: interfacing the token to a client computer (Cooper: page 1, paragraph 0018; page 2, paragraph 0042; Williams: page 5, paragraph 0042); and writing the certificate and the private key to the token across the network (Cooper: page 2, paragraph 0043).

As per claim 12, Cooper-Williams teaches the method of claim 4, wherein storing the certificate comprises: interfacing the token to a server computer (Cooper: page 2, paragraph 0042); and writing the certificate to the token at the server computer (Cooper: page 5, paragraph 0064).

As per claim 13, Cooper-Williams teaches the method of claim 5, wherein distributing data to the client comprises distributing a media player (Cooper: page 12, paragraph 0179).

As per claim 14, Cooper-Williams teaches a method for distributing data over a network comprising: establishing a secure connection between a client and a server (Cooper: page 2, paragraph 0032); receiving a request from the client for data to be downloaded (Cooper: page 2,

paragraph 0019); generating a message associated with the data being downloaded to the client and associated with a token used by the client (Cooper: page 8, paragraph 0102; Williams: page 5, paragraph 0042); and distributing the data and the associated message to the client (Cooper: page 8, paragraph 0110).

As per claim 15, Cooper-Williams teaches the method of claim 14, wherein establishing a secure connection comprises establishing a secure connection using a security protocol (Cooper: page 2, paragraph 0032).

As per claim 16, Cooper-Williams teaches the method of claim 15, wherein the security protocol is the secure socket layer protocol (Cooper: page 2, paragraph 0032).

As per claim 17, Cooper-Williams teaches the method of claim 14, wherein establishing a secure connection comprises requesting authentication information from the client (Cooper: page 8, paragraph 0126); and sending authentication information from the server (Cooper: page 5, paragraph 0057).

As per claim 18, Cooper-Williams teaches the method of claim 17, wherein requesting authentication information from the client comprises requesting a certificate from the client (Cooper: page 2, paragraph 0018); and requesting a digital signature from the client (Cooper: page 5, paragraph 0057; where the retrieving of a digital certificate includes the digital signature).

As per claim 19, Cooper-Williams teaches the method of claim 17, wherein sending authentication information from the server comprises sending a certificate from the server; and sending a digital signature from the server (Cooper: page 14, paragraphs 205-209).

As per claim 20, Cooper-Williams teaches the method of claim 18, wherein requesting a certificate comprises reading the certificate from the token used by the client (Cooper: page 11, paragraph 0163).

As per claim 21, Cooper-Williams teaches the method of claim 14, wherein generating a message further comprises: including in the message a data identification number (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102; where the watermark contains the identification number and message); including in the message a period of time for which the data may be used by the client (Williams: page 1, paragraph 0005); including in the message a distinguishing number of the token used by the client when requesting data (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); and including in the message a symmetrical key used to encrypt the data from the server to the client over the network (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102). Motivations to combine teachings are discussed in the treatment of claim 1.

As per claim 22, Cooper-Williams teaches the method of claim 14, wherein generating a message further comprises generating a message using a public key (asymmetric) cryptographic algorithm (Cooper: page 8, paragraph 0103).

As per claim 23, Cooper-Williams teaches a method of securely utilizing downloaded data comprising: opening a media player (Cooper: page 8, paragraph 0124); opening a data file (Cooper: page 8, paragraph 0124); requesting a token from a client (Cooper: page 2, paragraph 0018); reading a distinguishing number from the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); verifying a digital message associated with the data file and the token using the media player, the distinguishing number, and a private key in

the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102).

As per claim 24, Cooper-Williams teaches the method of claim 23, wherein in verifying a digital message, the media player reads the private key from the token to decrypt the digital message (Cooper: page 3, paragraph 0043).

As per claim 25, Cooper-Williams teaches the method of claim 23, wherein in verifying a digital message, the media player sends the digital message to the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102; where the whole watermarking process entails verification).

As per claim 26, Cooper-Williams teaches the method of claim 25 and the use of a public key to decrypt an encrypted symmetric key, but does not specifically teach the token's decryption of an encrypted symmetric key using the private key. It would have been obvious to one of ordinary skill in the art at the time of the invention to include the functionality of the use of a private key to decrypt an encrypted symmetric key, as it is well known in the art. (See: Fischer, U.S. 5,436,972; column 12, lines 36-45, for example). Also, the use of a private key to decrypt, over the use of a public key is a design choice, and is thus not patentably distinct.

As per claim 27, Cooper-Williams teaches the method of claim 22, wherein verifying a digital message comprises verifying the distinguishing number read from the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); verifying a time period associated with the data file (Williams: page 1, paragraph 0005); decrypting an encrypted symmetrical key using the private key from the token; and decrypting the data file using the symmetrical key (see discussion of claim 26).

As per claim 28, Cooper-Williams teaches a system for distributing data over a network comprising: a client computer for requesting data over a network, the client computer being interfaced to the network (figure 1); a server computer for distributing requested data over a network, the server computer being interfaced to the network (figure 1); and a token interfaced to the client computer (Cooper: page 2, paragraph 0018; Williams: page 5, paragraph 0042), wherein the server computer stores a certificate and a private key in the token (Cooper: page 17, paragraph 0277).

As per claim 29, Cooper-Williams teaches the system of claim 28, wherein the server computer verifies an identity of the client with the certificate in the token before distributing data to the client (Cooper: page 2, paragraph 0019).

As per claim 31, Cooper-Williams teaches a system for distributing data over a network comprising: a client computer for requesting data over a network, the client computer interfaced to the network (Cooper: figure 1); a server computer for distributing requested data over a network, the server computer interfaced to the network (Cooper: figure 1); and a token interfaced to the client computer (Cooper: page 2, paragraph 0018; Williams: page 5, paragraph 0042). Cooper-Williams does not specifically teach a third party computer system interfaced to the network that issues certificates and stores tokens. It would have been obvious to one of ordinary skill in the art at the time of the invention to include this limitation. Since in Cooper-Williams teaching, the capability exists to issue certificates and storing them in the token, having a third-party storage computer constitutes a design choice and would thus have been obvious to one of ordinary skill in the art.

As per claim 32, Cooper-Williams teaches the method of claim 31 on the basis of obviousness but does not specifically teach that the third party computer issues a private key and stores the private key in the token. It would have been obvious to one of ordinary skill in the art at the time of the invention to include this limitation. Since Cooper-Williams teaches the issuance and storage of a private key in a token, using a third party computer to achieve this end constitutes a design choice and would thus have been obvious to one of ordinary skill in the art.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper-Williams in view of Fanning (U.S. 6,742,023).

As per claim 30, Cooper-Williams teaches the system of claim 28, further comprising a cryptographic processor interfaced to the server computer (where the existence of the processor is obvious, given the invention's cryptographic ability, as previously discussed). Cooper-Williams does not specifically teach the existence of a firewall interfaced to the network. Fanning teaches this limitation (Fanning: figure 5). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a firewall interfaced to the network, as taught by Fanning in the system of Cooper-Williams. The motivation for doing so lies in the fact that there exists a need to account for firewalled nodes to provide further security to the invention. Adding this firewall component enables further safety and adds functionality to the invention as well. All teachings are from the same field of endeavor, namely the safe transmission of data files over a network.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Cooper et al. (U.S. 2002/0029350) teaches a web based conferencing network.

b. Toh et al. (U.S. 2002/0004902) teaches a secure and reliable document delivery.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tanim Hossain whose telephone number is 571/272-3881. The examiner can normally be reached on 8:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571/272-3880. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tanim Hossain
Patent Examiner
Art Unit 2145

JACK B. HARVEY
SUPERVISORY PATENT EXAMINER